كتيبة الترجمة في كتائب غزو الإنترنت الجهادية

تقدم:

ترجمة لسلسة مقالات عن حرب الشبكات المعلوماتية

The Economist

1 July 2010

Cyberwar: War in the fifth domain

Are the mouse and keyboard the new weapons of conflict?

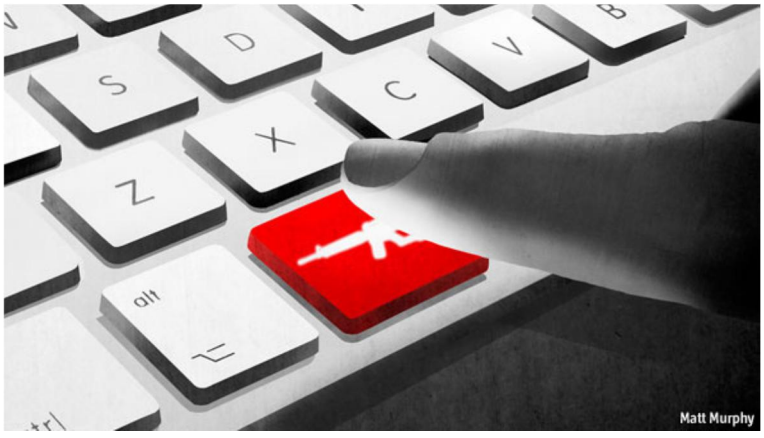
http://www.economist.com/node/16478792

الإيكونوميست

١ يوليو/تموز 2010

حرب الشبكات المعلوماتية: حرب الميدان الخامس

الفأرة ولوحة المفاتيح، هل هما السلاحان الجديدان في المعركة؟



اكتشف قمر صناعي أمريكي انفجاراً هائلاً في سيبيريا في شهر حزيران/يونيو سنة 1982، وذلك في ذروة الحرب الباردة. هل كان إطلاق لصاروخ؟ أم تجربة نووية؟ كأنه كان انفجار لخط سوفييتي للغاز. وكان السبب هو خلل في نظام التحكم الإلكتروني الذي سرقه الجواسيس السوفييت من شركة في كندا. لم يعرف هؤلاء أن وكالة المخابرات المركزية الأمريكية (CIA) كانت قد عبثت بالبرامج الحاسوبية لنظام التحكم هذا فيما يجعله يتصرف بطريقة عشوائية بعد فترة من الوقت، فيقوم بزيادة سرعة المضخات وتغير تركيبات الصمامات لكي تنتج ضغوط اعلى بكثير مما تستطيع اللحامات والمفاصل أن تتحمله، هذا وفقاً لمذكرات توماس ريد (السكرتير العام السابق لسلاح الجو الأمريكي) الذي قال "أن النتيجة كانت اكبر انفجار غير نووي واكبر نار تشاهد من الفضاء".

كان هذا استعراضا لقوة قنبلة جديدة تسمى ب "قنبلة المنطق". بعد ذلك بثلاث عقود، ومع ازدياد عدد أجهزة الحاسبات الآلية المرتبطة على الشبكة الإلكترونية، هل يستطيع أحد أن يستعمل قنبلة المنطق ليطفئ الكهرباء في الجانب الآخر للعالم؟ هل يستطيع الإرهابيون أو مخترقوا الشبكات الإلكترونية أن يسببوا أزمة مالية عشوائية في بورصة نيويورك إذا عبثوا في أجهزة تبادل الأسهم المبرمجة إلكترونياً؟ وبما أن رقاقات وبرامج الحاسبات الآلية مصنعة عالمياً، فهل باستطاعة قوة دخيلة أن تلوث المعدات العسكرية المتفوقة تقنياً بالفيروسات؟ قال مصدر عسكري أمريكي رفيع "إنه امر يرعبني للغاية، فالمقدرة التدميرية عظيمة جداً".

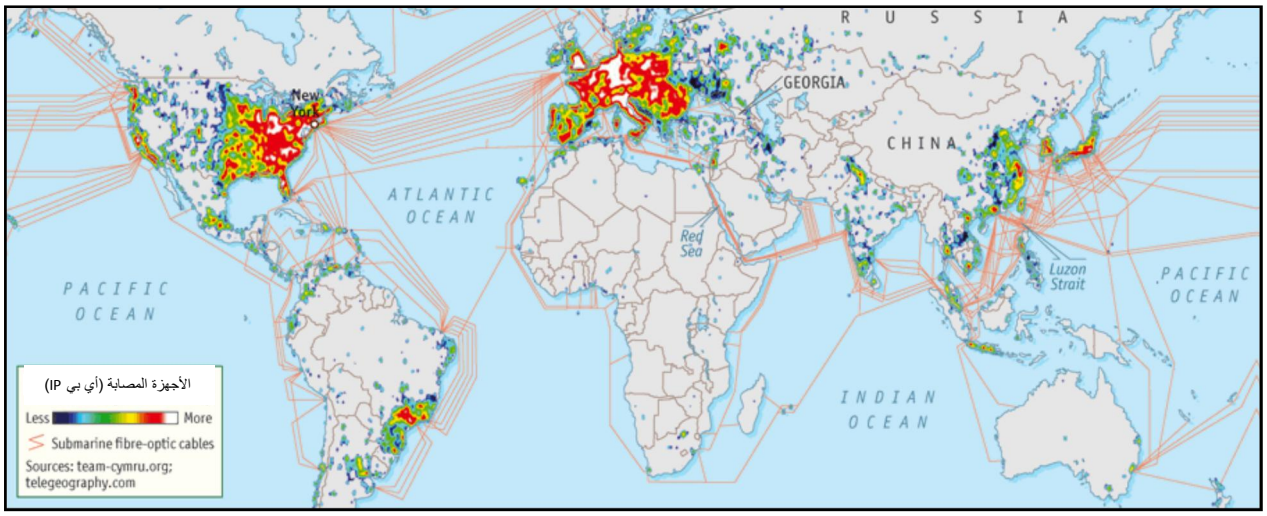
دخلت حرفة الحرب ميدانها الخامس بعد ميادين الأرض، والبحر، والجو، والفضاء، جاء ميدان الشبكات المعلوماتية. فقد أعلن الرئيس الأمريكي باراك أوباما أن البنية الرقمية الأمريكية هي ثروة وطنية استراتيجية، وقام بتعيين هاورد شميت رئيس أمن شركة مايكروسوفت السابق مديرا للأمن الإلكتروني. وقام البنتاغون في شهر أيار الماضي بأنشاء مركز قيادة شبكة المعلومات الجديد (CYBERCOM) برئاسة الجنرال كيث الكسندر، مدير هيئة الأمن الوطنية (Homeland Security). مهمة المركز أن يقوم بعمليات شاملة للدفاع عن الشبكات الإلكترونية العسكرية الأمريكية، وان يهاجم شبكات البلدان الأخرى. ولكن تبقى ماهية وكيفية العمليات سرية.

قامت بريطانيا أيضا بتعيين طاقم أمن إلكتروني وأنشاء مركزاً للعمليات مقره في (LGCHQ)، وهو الموازي البريطاني لهيئة الأمن الوطنية (Homeland Security) في أمريكا. وتتكلم الصين عن أنها ستربح حروب معلوماتية في منتصف القرن الواحد والعشرين. وعدد كبير من الدول تتهيأ للحرب على الشبكات المعلوماتية، منها روسيا، والكيان الصهيوني، وكوريا الشمالية. كما تفتخر ايران بأن لديها ثاني اكبر جيش إلكتروني في العالم.

ما هو الشكل الذي ستتخذه تلك الحرب الإلكترونية؟ يتصور ريتشارد كلارك الموظف السابق في البيت الأبيض الذي كان مسؤولاً عن محاربة الإرهاب وعن الأمن الإلكتروني في كتاب جديد له، يتصور فشلاً فادحاً خلال 15 دقيقة. هدم فيروسات الحاسبات الآلية لأنظمة البريد الإلكترونية العسكرية، تفجير مصافي وأنابيب بترول، انهيار أنظمة توجيه الطائرات، خروج قطارات الشحن والركاب عن سككها، تسرب المعلومات المالية، توقف شبكة الكهرباء في شرقي الولايات المتحدة، التفاف عشوائي للأقمار الصناعية، انهيار المجتمع نتيجة عدم توفر الطعام واستهلاك المال، والأسوأ من هذا كله أن هوية المهاجم ممكن أن تبقى غامضة.

في نظر مايك ماكدونالد (أحد قادة التجسس سابقاً) أن تأثير هجوم إلكتروني عالمي شبيه جداً بهجوم نووي، ويقول أن الحرب الإلكترونية العالمية قد بدأت "وأمريكا تخسرها". وعلى صعيد أخر يقول السيد شميدت: " أن الأمر ليس كذلك، ليس هناك حرباً إلكترونية عالمية". ويتهم بروس شنايدر (خبير علم أمن التكنولوجيا) المنتفعين من الحرب الإلكترونية كالسيد كلارك بترويج الذعر. فهو يقول أن العالم الإلكتروني سيكون بالتأكيد جزءاً من أية حرب في المستقبل، ولكن هجوم مروع كهذا على أمريكا صعب أن يتحقق وهو شيء من محض الخيال ومعقول فقط في إطار حرب حقيقية وفي هذه الحال فمن الأرجح أن يكون المعتدي معروف.

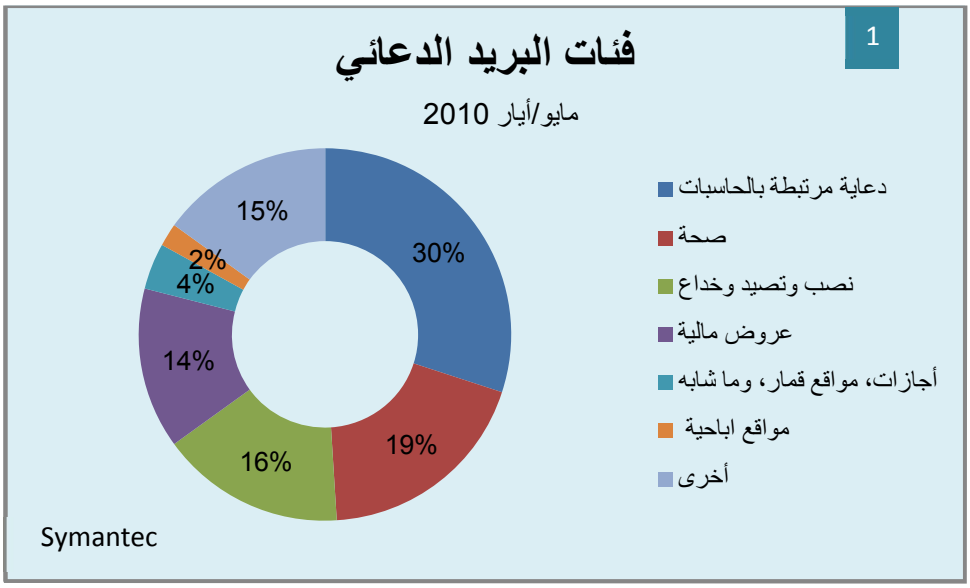
إن علم الحاسبات للقادة العسكريين هو بركة ولعنة لهم. فالقنابل الموجهة بنظام التموضع العالمي؛ والطائرات دون الطيار تطير بسيطرة لاسلكية عبر العالم؛ والطائرات المقاتلة والسفن أصبحت الآن مراكز ضخمة لتحليل المعلومات؛ حتى جندي المشاة العادي اصبح الآن متصلاً بتلك الشبكات. ولكن ازدياد التواصل على شبكة غير آمنة يضاعف من طرق الهجوم الإلكتروني عليها. وازدياد الاتكال على الحاسبات يزيد من تلك الأضرار.



تستطيع شبكات المعلومات أن تجزء المعلومات وأن تبثها عبر طرق متعددة مما يقلل من فقدان أجزاء كبيرة من هذه الشبكات. ولكن بعض البنية الرقمية العالمية قد تتأثر بصورة أكبر، إذ أن أكثر من 90% من حركة المرور في شبكة المعلومات (مثل الإنترنت) تنتقل عبر خطوط ألياف ضوئية ممدودة تحت البحار. وهذه الخطوط مجمعة بخطورة في نقاط قليلة ضيقة حول نيويورك، أو البحر الأحمر أو مضيق لوزون في الفيليبين (أنظر الخريطة) تُوجه حركة مرور تلك الشبكة بواسطة 13 ملقم من خادمات أسماء النطاق الضعيفة (domain-names servers)، وهناك مخاطر أخرى قادمة. فمساحات شاسعة من أفريقيا التي فيها حكومات ضعيفة، تُوصل الآن بخطوط ألياف بصرية مما يشكل ملاذاً جديداً لمرتكبي الجرائم المعلوماتية. وانتشار الشبكات الجوالة سيتيح فرص جديدة للاختراق.

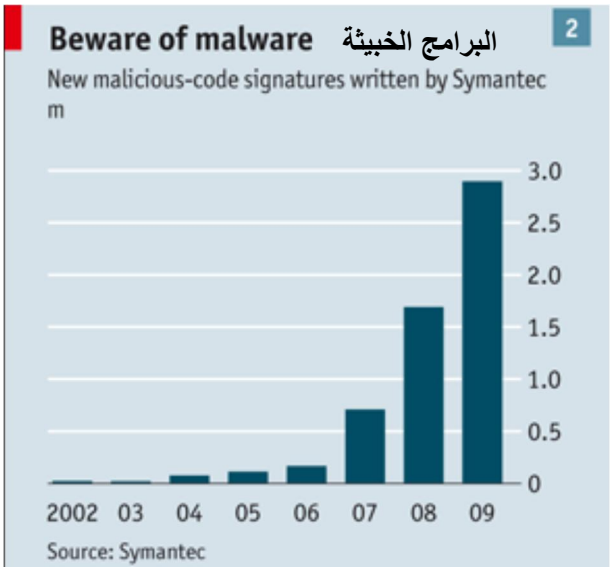
شبكة المعلومات كانت قد صممت للسهولة وليس للأمن. ولكن في توصيل العالم ببعضه البعض اختلطت الحدائق مع الغابات فجواز السفر غير مطلوب في عالم الإنترنت. بينما الشرطة محددة الحركة بالحدود الدولية فأن مرتكبي تلك الجرائم يتحركون بحرية. لم تعد الأمم المعادية عبر البحار بل هي خلف الجدار الناري للحاسب الآلي ويستطيع ذوي النوايا السيئة أن يحجبوا معرفاتهم وأماكنهم، وان يقلدوا الآخرين، وان يدخلوا باحتيال على الأبنية التي تحتوي على الثروات الرقمية للعصر الإلكتروني: المال، والمعلومات الشخصية، والممتلكات الفكرية.

قدر أوباما خسائر الجرائم المعلوماتية بترليون دولار، عالم خفي أكبر من عالم تجارة المخدرات. مع أن هذه الأرقام مختلف عليها، فالمصارف والشركات لا ترغب في أن تقر بكمية المعلومات التي تفقدها. فقد سجلت شركة فيرايزون للاتصالات (Verizon) فقدان 285 مليون سجلاً شخصياً في عام 2008 وحده، بما فيه تفاصيل بطاقات اعتماد، وحسابات مصرفية، خلال تحقيقات أجرتها لزبائنها.



يُكون البريد الدعائي (Spam) 90% من ال 140 مليار بريد إلكتروني المرسلة يومياً؛ و 16% من ذلك يحتوي على مشاريع غير شرعية للحصول على الأموال. (أنظر اللائحة 1) بما فيها رسائل التصيد (phisihing) التي تسعى إلى خداع مستلميها لأن يعطوا كلمات مرورهم وتفاصيل معلوماتهم المصرفية (صدر ذلك عن سيمانتيك أحدى شركات أمن الحاسبات الآلية). أن كمية المعلومات الشخصية المتوفرة على الشبكة الآن سهلت جداً مهاجمة الحاسبات الآلية، وذلك بواسطة افتعال بريد شخصي يمكن الثقة به وفتحه. هذا ما يعرف "بالتصيد بالرمح".

مخترقوا الحاسبات الآلية ومبرمجي الفيروسات الذين عبثوا في الحاسبات الآلية سابقاً للمرح فقط قد ذهبوا واستبدلوا الآن بزمر من مرتكبي الجرائم يسعون إلى جمع المعلومات. يقول غريغ ديي من ماكافي (أحدى شركات أمن الحاسبات الآلية) أن الغرض من الاختراق في الماضي كان لإحداث ضجة، أما اليوم فالهدف هو الصمت. أصبح مخترقوا الحاسبات الآلية موزعي جملة للبرمجيات الخبيثة (Malware) والفيروسات والدودة وأحصنة طروادة التي تصيب الحواسيب، ليتمكن الآخرون من استعمالها. وأصبحت مواقع الإنترنت هي الأماكن المفضلة لنشر تلك البرمجيات الخبيثة لان الغافل قد يوجه إليها من خلال إعلانات دعائية أو روابط تنشر على مواقع التعارف الاجتماعي. والمواقع المصممة لأغراض الخداع والتصيد التي غالباً ما توفر منفذاً إلى المعلومات الثمينة.



إن أرقام البرمجيات الخبيثة (Malware) تتضاعف (انظر إلى اللائحة 2) إنها تستعمل عادة لسرقة كلمات المرور، ومعلومات أخرى. أو لتفتح "باباً خلفياً" في الحاسبات حتى يتمكن الاستيلاء عليها من قبل دخلاء. هذه الأجهزة المصابة (Zombies) يمكن أن ترتبط بالآلاف إذا لم يكن بالملايين من الأجهزة حول العالم، مما يشكل ما يسمى بالبوت نت (Botnet). التقديرات لعدد الأجهزة الملوثة يتراوح المئة مليون. (راجع خارطة انتشار التلوث في العالم) تستعمل شبكات البوت نت لإرسال البريد الدعائي (Spam)، نشر البرمجيات الملوثة (Malware)، أو شن هجومات نكران الخدمة (DDoS) والتي تسعى إلى تعطيل جهاز أو موقع مستهدف عن طريق تحميله بعدد لا يحصى من الطلبات الزائفة فيتوقف عن العمل.

الجاسوس الذي ضللني

يفتش المجرمون عادة على فريسة سهلة. ولكن الدول التي تريد أن تمارس هكذا جرائم تستطيع أن توفق ما بين طرق الاختراق (كالتصيد بالرمح) وأجهزة استخباراتها للتجسس على هدف ما عن طريق فك الشفرات والوصول إلى كلمات المرور والمثابرة على اقتحام جهاز أو موقع حتى تجد فيه نقطة ضعف. يقول ستيفن شابنسكي (وهو مسؤول رفيع في مكتب التحقيقات الفيدرالية الأمريكية (FBI)): **"**أنه إذا توفر الوقت الكافي، **و**الدافع والتمويل لشخص ذو تصميم، فسينجح دائماً في اختراق الجهاز أو الموقع المستهدف".

يخاطر الجواسيس التقليديين بالاعتقال أو القتل عندما يحاولون أن يهربوا نسخاً من الوثائق، ولكن أقرانهم في العالم الإلكتروني لا يواجهون مثل هذه المخاطر. فقد قال مصدر عسكري أمريكي رفيع: "أنه كان من الممكن لجاسوس أن يُهرب ما يعادل بضعة كتب من الوثائق في الماضي، أما الآن في عالم اختراق شبكات المعلومات فيأخذون المكتبة كلها وإذا رتبت الرفوف مجدداً فسيستولون عليها ثانية".

تُتهم الصين خاصة بالتجسس الشامل، حيث تهاجم الحاسبات الآلية لمتعهدي الدفاع الغربي، ومن المعتقد أنها استولت على تفاصيل سرية لطائرة F35 المقاتلة (الركن الأساسي للقوة الجوية الأمريكية) ويعتقد بأنها استهدفت غوغل وحفنة أخرى من شركات تكنولوجيا الإنترنت في نهاية 2009. يقول خبراء في أمن المعلومات في شركة لوكهيد مارتن (وهي شركة مقاولة لوزارة الدفاع الأمريكية التي تنفي تضييع معلومات ال F 35) في ولاية ماريلاند: "أنه من الصعب التصدي للهجمات المستمرة المتقدمة التي تستهدف ما لا يحصى من مداخل شبكاتها". يحاول المخترقون أحيانا أن يسربوا المعلومات ببطء مخبئة في مجرى سير الإنترنت العادي وحاولوا في بعض الأحيان أن يدخلوا بترك وحدات تخزين (memory-stick) ملوثة في موقف سيارات العاملين في الشركة آملين أن يجدها احد ما ويضعها في حاسبه. ويجب الإشارة إلى أن رسائل البريد الإلكترونية حتى الغير سرية تحتوي على ثروة من المعلومات المفيدة عن مشاريع في مرحلة الإنشاء.

يقول جيم لويس من مركز الدراسات الاستراتيجية (وهو عبارة عن مؤسسة فكرية في واشنطن العاصمة): "إن تجسس الإنترنت هو اكبر كارثة استخباراتية منذ سرقة الأسرار النووية في أواخر الأربعينيات، ومن الممكن أن يكون هذا النوع من التجسس الأكثر خطورة على الغرب. فقد تؤدي خسارة المعرفة التكنولوجيا العالية إلى خسران التفوق الاقتصادي، وأثلام الحد العسكري إذا وصلت المسألة إلى حرب فعلية".

يعتقد جواسيس الغرب أن الصين تستخدم مخترقي شبكات أكثر مواظبة وجراءة ، ولكن نظرائهم الروس هم أكثر مهارة ودقة. ويقولون أن هيئة الأمن الوطنية الأمريكية وقيادة الاتصالات الحكومية البريطانية لا يزالا في مقدمة المجموعة، الأمر الذي يفسر سبب عدم تذمر الدول الغربية من اختراق الشبكات إلا حديثاً.

الخطوة الثانية بعد أن تخترق الشبكات لسرقة المعلومات، هي عرقلتها والتحكم بها. فاذا كان من الممكن مهاجمة معلومات التهديف العسكرية، فالصواريخ العابرة للقارات (مثلاً) تصبح دون منفعة. ويتحدث المشاركين في المناورات الحربية عن تغيير النقط الحمراء والنقط الزرقاء وعن جعل القوات الموالية (زرقاء) تبدو وكأنها معادية (حمراء) والعكس صحيح للتمويه.

يقول الجنرال الكسندر أن البنتاغون وهيئة الأمن الوطنية بدءا بالتعاون في حرب العالم الإلكتروني في أواخر 2008 بعد "اختراق جديّ لشبكاتنا السرية". ويقول السيد لويس أن في هذا إشارة إلى اختراق القيادة المركزية (Central Command) التي تشرف على الحروب في العراق وأفغانستان بواسطة وحدة تخزين ملوثة. لا يعرف أحد إذا حصل أي ضرر أو إلى أي مدى، ولكن مجرد فكرة تربص العدو بتلك الأنظمة هو أمر مرعب لهؤلاء القادة.

بعد كل هذا من الممكن للمخترق أن يقتحم أجهزة التعبئة والتموين الغير سرية أو حتى البنية المدنية. وفقدان الثقة بالبيانات المالية والحوالات الإلكترونية قد يسبب اضطراب اقتصادي. والقلق الأكبر من ذلك هو اقتحام للشبكة الكهربائية، فليس من العادي أن تحتفظ شركات الكهرباء بقطع غيار باهظة الثمن للمولدات الكهربائية في مخازنها والتي تتطلب عملية استبدالها شهور، ولا تستطيع مولدات الديزل أن تستكمل ما فقدته الشبكة الكهربائية كما أنها لا تستطيع أن تعمل للأبد. فبدون الكهرباء والخدمات الأخرى الماسة ستتوقف أجهزة الاتصالات وأجهزة الصرف الآلي عن العمل. ويقدر البعض أن فقدان الكهرباء لأيام قليلة قد يؤدي إلى دمار اقتصادي تسلسلي.

يختلف الخبراء على ضعف الأجهزة التي تشغل المعامل الصناعية المعروفة بالتحكم الإداري وجمع المعلومات (SCADA). ولكن المزيد من هذه الأجهزة ترتبط بالإنترنت، مما يزيد من خطورة الهجمات المتحكم بها عن بعد.

تقوم شركات تصنيع الشبكات الذكية (Smart Grids) (التي توصل معلومات حول معدل استهلاك الطاقة لشركات الطاقة) بالدعاية لمنتجاتها على أنها وسائل لتخفيض تبذير الطاقة، ولكنها تزيد من احتمالات ارتكاب جرائم (كتزوير الفواتير مثلاً) وتعرض شبكات التحكم الإداري وجمع المعلومات (SCADA) للاختراق.

وتحدث الجنرال الكسندر عن إشارات تفيد أن بعض الاختراقات تستهدف أجهزة للتخريب من بُعد ولكن ما يحصل بالضبط غير واضح. هل يتحسس الدخلاء أنظمة (SCADA) للاستكشاف فقط؟ أم لفتح باب خلفي لاستعماله في المستقبل؟ وقال مصدر عسكري أمريكي أنه إذا تبين أن أية دولة تزرع قنبلة منطقية في الشبكة الكهربائية فسيعتبر هذا استفزازاً يعادل أزمة الصواريخ الكوبية.

إستونيا، جورجيا والحرب العالمية الأولى

يجري الآن أعادة التفكير في مبادئ التعبئة والقوانين الخاصة بحرب الشبكات المعلوماتية وذلك في معسكر سوفييتي سابق في إستونيا، وهو الآن مقر الناتو (NATO) للدفاع عن الشبكات المعلوماتية. ولقد تأسس رداً على ما اصبح معروفاً بحرب الوب 1 (Web War 1). وتلك الحرب كانت هجمات منسقة لتعطيل الخدمات شنت على الحكومة الإستونية والأجهزة الإعلامية وشبكات أحد المصارف التي نقلت رمزاً تذكارياً من العهد السوفييتي من وسط تالين في عام 2007. وقد كان هذا اضطراب إلكتروني اكثر مما كان حرباً، ولكنه أجبر الحكومة الإستونية على أن تقطع خدمة الإنترنت.

ظهرت هجمات مماثلة خلال حرب روسيا مع جورجيا في السنة اللاحقة، ظهرت وكأنها كانت منسقة مع تقدم الصفوف العسكرية الروسية. فقد تعطلت مواقع الإنترنت الحكومية والصحفية وازدحمت خطوط الهواتف مما أضعف مقدرة جورجيا في أن تسمع البلدان الأخرى صوتها وتعرض عليهم قضيتها. وقد نُقل الموقع الإلكتروني للرئيس الجورجي ميخائيل ساكاشفيلي إلى خادم (Server) أمريكي اكثر قدرة على صد الهجوم وذهب خبراء من إستونية إلى جورجيا لمساعدتها.

يعتقد الكثيرون أن التحريض على هذه الاعتداءات جاء من الكرملين. ولكن التحقيقات تتبعت جذورها إلى "ناشطي الاختراقات" الروس والبوت نت الغير شرعية، وأن عدداً كبيراً من تلك الحاسبات كانت في بلدان غربية. وهذا العمل فتح المجال لأسئلة جديدة مثل: هل الهجوم الإلكتروني على إستونيا وهي عضو في حلف الناتو يعتبر هجوماً مسلحاً؟ وهل كان من الموجب على الحلف أن يدافع عنها؟ وهل مساعدة إستونيا لجورجيا (وهي ليست عضواً في حلف الناتو) قد يؤدي إلى أدخال إستونيا في حرب وبالتالي أدخال حلف الناتو معها؟

تخللت أسئلة كهذه مناقشات المفهوم الاستراتيجي الجديد لحلف الناتو الذي سيتبنى أواخر هذا العام (2010). وأفادت لجنة من الخبراء (على رأسهم مادلين أولبرايت وزيرة الخارجية الأمريكية السابقة) في شهر مايو/أيار الماضي أن الهجمات الإلكترونية تشكل خطراً واحداً من اصل ثلاثة أخطار اكثر احتمالاً أن تهدد الحلف. وقالت اللجنة أن الهجوم القادم إن كان مميزاً ومن الممكن أن يكون جدّي لدرجة أن يتطلب رداً بناءً على البند رقم 5 من قوانين الدفاع المتبادل (والتي تنص على أن هجوم على أحد أعضائها هو هجوم على الكل يستدعي رداً مناسباً).

أرسل أعضاء مجلس الشيوخ الأمريكي إلى الجنرال الكسندر خلال جلسة تعيينه عدة أسئلة. هل سيكون لديه أسلحة إلكترونية هجومية ملحوظة؟ هل سيشجع وجود هذه الأسلحة آخرين أن يتبعوا ذات المنهج؟ ما هي درجة التأكد من هوية المعتدي الضرورية قبل أن يقوم بالرد؟ حُفظت الأجوبة لهذه الأسئلة في ملف سري، وقال الجنرال علناً أن الرئيس هو صاحب القرار في ما يمكن اعتباره حرباً إلكترونية وإذا ردت أمريكا مستخدمة قوة عسكرية فسيكون هذا تبعاً لقوانين الحرب ومبادئ الضروريات العسكرية والتمييز والتناسب.

استغراق عملية تعيين الجنرال الكسندر سبعة اشهر يدل على المخاوف التي شعر بها أفراد مجلس الشيوخ تجاه دمج المهمات العسكرية مع العمليات التجسسية. والمخاوف أن عسكرة العالم الإلكتروني قد تتعدى على الحريات الخاصة للأمريكيين.

ستحمي قيادة حرب الشبكات المعلوماتية (Cyber-command) نطاق الإنترنت العسكري المنتهي ب (mil) ونطاق الحكومة (gov) والبنية التجارية (com) التي ستندرج تحت مسؤولية دائرة الأمن الوطني (Homeland Security) والشركات الخاصة على التوالي بدعم من قيادة حرب الشبكات المعلوماتية (Cyber-command).

يقول مسؤول عسكري رفيع أن أولويات الجنرال الكسندر هي تطوير دفاعات الشبكات العسكرية، فيما يلقي مسؤولاً آخر الشك حول الهجوم الإلكتروني، فيقول: "من الصعب أن يتم في وقت معين. أذا أُستعمل الهجوم الإلكتروني كسلاح عسكري، فما تريده هو وقت وتأثير معروفان. وإذا كنت تستعمله للتجسس، فلا أهمية، لأنه يمكنك الانتظار". ثم يلمح أن يستعمل السلاح الإلكتروني كسلاح إضافي إلى سلاح تقليدي في ساحة محدودة.

من الممكن أن الصينيون يفكرون بنفس الطريقة. فقد ذكر في تقرير عن الحرب الإلكترونية الصينية كتب إلى اللجنة التحضيرية المخولة بدراسة العلاقات الاقتصادية والأمنية بين الولايات المتحدة والصين، أن الصين تستعمل الأسلحة الإلكترونية ليس لتهزم أمريكا ولكن لتعرقل وتبطأ قواتها مدة كافية، لتتمكن الصين من احتلال تايوان دون أن تخوض حرباً قتالية.

الإبادة أو التباين؟

دعنا نقول أن استراتيجية الدفاع في الحرب الإلكترونية هي أقل فعالية من الاستراتيجية النووية. فليس هناك دمار أكيد ومتبادل والخط الفاصل بين الجريمة والحرب خط غير واضح، وكذلك صعوبة معرفة المعتدي. لا يجوز أن يكون الرد محصور على العالم الإلكتروني، فالنظام الوحيد الذي بالتأكيد ليس متصلاً بشبكة الإنترنت العامة هو نظام سلسلة إطلاق الصواريخ النووية الأمريكية، ومع ذلك فإنه من الأرجح استعمال الأسلحة الإلكترونية ليس للتدمير الإلكتروني الشامل بل كأداة حرب محدودة.

تكون الأسلحة الإلكترونية اكثر فعالية في أيدي الدول الكبرى، ولكن لأنها رخيصة فمن الممكن أن تكون اكثر فائدة لمن هو أقل قوة، فمن الممكن أن تلائم الإرهابي. ربما من حسن الحظ، أن القاعدة وغيرها من التنظيمات الجهادية استعملوا الإنترنت لغرض الدعاية والاتصالات فقط حتى الأن. ومن المحتمل أن المجاهدين لا يملكون حالياً القدرة التقنية لتفجير مصفاة للبترول عن طريق اختراق شبكتها. أو انهم في الوقت الحاضر يفضلون التفجيرات الاستشهادية على التخريب الإلكتروني السري.

مع تحيات إخوانكم في

كتائب غزو الإنترنت الجهادية